

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

the premises located at 7603 Sessis Drive, Columbus, Ohio

Case No.

2:20-mj-454

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
7603 Sessis Drive, Columbus, Ohio being a two-story, single family residence with an attached garage. "7603" is posted above the front door. The front door is white with light green trim around it. The exterior is tan vinyl siding. The windows have dark green shutters.
located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1956; 21 U.S.C. § 846; 21 U.S.C. § 841;	Laundering of Money; Conspiracy to Possess with Intent to Distribute a Controlled Substance; Possession with Intent to Distribute a Controlled Substance;
21 U.S.C. § 856; 21 U.S.C. § 843(b)	Maintaining a Drug-Involved Premises; Use of a Communication Facility to Commit a Federal Drug Felony

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date:

6-26-20

City and state: Columbus, Ohio

TFO [Signature]

Applicant's signature

TFO Andrew Wuerz

Printed name and title

[Signature]

Judge's signature

Magistrate Judge Chelsey Vasquez

Printed name and title



II. DESCRIPTION OF PROPERTY TO BE SEARCHED

5. **Subject Premises 1:** 7603 Sessis Drive, Columbus, Ohio being a two-story, single family residence with an attached garage. “7603” is posted above the front door. The front door is white with light green trim around it. The exterior is tan vinyl siding. The windows have dark green shutters.

6. **Subject Premises 2:** 7772 Deercrest Court, Dublin, Ohio being a two-story, condominium residence. “7772” is posted to the left of the front door. The front door is green with tan trim around it. The windows have green shutters. The first floor exterior is brick. The second floor exterior is tan vinyl siding.

III. BASIS FOR PROBABLE CAUSE

7. Arizona has a Joint Task Force consisting of federal agents in the Drug Enforcement Administration (DEA), United States Postal Inspection Service (USPIS), the Internal Revenue Service Criminal Investigations (IRS), and Homeland Security Investigations (HSI) investigating domestic and international drug trafficking activities of Darknet marketplace vendors who utilize the internet to facilitate the sale, transportation, and distribution of illegal drugs throughout the United States.

8. In early November 2019, the task force learned of a Darknet vendor using the moniker “livedabs” suspected of mailing parcels containing narcotics from the Phoenix, Arizona metropolitan area throughout the United States. Though undercover purchases, surveillance and intercepted parcels, agents in Arizona identified Rachel Rempel (REMPEL) and Charles McCoy (MCCOY) as mailers of packages containing narcotics associated with livedabs. Agents have also discovered through undercover purchases and intercepted parcels, that livedabs packages their narcotics similarly—in vacuum sealed and/or mylar bags containing a yellow, mustard like substance with an odor similar to Bengay. The packages also tend to contain return addresses of legitimate businesses that have no association with REMPEL, MCCOY, or any co-conspirator identified to date. As

the investigation continues to develop, agents have identified additional suspected co-conspirators, including Brandon Dirke (DIRKE) and Niesha Graves (GRAVES), both of whom reside in Ohio. Their actions and suspected criminal activities will be described below.

9. In December 2019, postal inspectors in Columbus, Ohio identified 19 outbound Priority Mail Express parcels as suspicious. The parcels all had a return address of "Bliss Life + Style, 4345 W Dublin Granville Rd, Dublin, OH 43017-2041" and were addressed to locations throughout the United States. One package was retained for further investigation (the "Bliss Parcel").

10. On December 27, 2019, postal inspectors traveled to Bliss Life + Style at 4345 West Dublin Granville Road, Dublin, Ohio 43017, and determined it to be a legitimate business. Inspectors spoke with the manager at the business about the Bliss Parcel. The manager stated she did not mail the parcel, did not believe any of the other employees at the business had mailed it and gave inspectors permission to open the parcel. The package was opened and found to contain approximately 30 gross grams of suspected powder cocaine inside a vacuum sealed bag coated with a mustard like substance.

11. A review of USPS databases identified a total of 129 parcels using the same return address as the Bliss Parcel. The labels for 113 of the 129 parcels were generated between December 26, 2019, and December 29, 2019. Of the 16 labels generated before that time, all but two were delivered to addresses in the greater Phoenix, Arizona area including Chandler, Scottsdale, Tempe, and Phoenix, Arizona.

12. MCCOY was found to be associated with at least two of the addresses in the Phoenix area that have been used to ship or receive packages. While MCCOY currently lives in Arizona, he used to live in the Columbus, Ohio area, and is related to GRAVES, who lives in Dublin, Ohio. USPS records indicate between September 2019 and the present, at least eight parcels originating in central Ohio have been delivered to these

addresses in the greater Phoenix, Arizona area. Return addresses utilized for these parcels were found to be either Morgan House, 5300 Glick Rd, Dublin, Ohio 43017, or Bliss Life + Style, 4345 West Dublin Granville Road, Dublin, Ohio 43017. The Morgan House is a restaurant, and similar to Bliss Life + Style, does not appear to be associated with MCCOY, REMPEL, DIRKE, GRAVES, or the other potential co-conspirators identified thus far.

13. In addition to the consent search described above, during the course of this investigation, agents in Arizona have obtained search warrants for two packages bearing the return address of Bliss Life + Style 4345 W Dublin Granville Road, Dublin, Ohio 43017, and found them to contain cocaine, fentanyl, and/or U.S. currency.

14. On January 27, 2020, surveillance video captured a female mailing a package from the Dublin post office in Dublin, Ohio, addressed to "Hold for Guest Rachal Rampal, 5101 N Scottsdale Rd, Scottsdale AZ 85250," with a return address of "Morgan House, 5300 Glick Rd, Dublin, OH 43017." Based on the investigation to date, Your Affiant believes this is a misspelling for Rachel REMPEL, a suspected co-conspirator and individual identified by agents in Arizona as a mailer of packages containing drugs for livedabs.

15. On January 30, 2020, surveillance video captured a female mailing a package from the Powell, Ohio post office. This parcel was addressed to "Hold for Jon Barnhill, 3560 N Marshall Way, Scottsdale AZ 85251," with the same return name and address of "Morgan House, 5300 Glick Rd, Dublin, OH 43017." Agents obtained a copy of and reviewed GRAVES' Ohio driver's license. The photograph on GRAVES' driver's license appears to be the same female who mailed the packages on January 27 and January 30, 2020.

16. On February 3, 2020, a U.S. Postal Inspector identified a package similar to previously seized packages. An image of the parcel showed the parcel was addressed to "HOLD FOR: JASMIN WILLIAM, 7490 VANTAGE DR, COLUMBUS OH 43235-

1416.” 7490 Vantage Drive is the address for a Hyatt Place hotel. Postal records indicate this parcel reached the Hyatt Place hotel at approximately 11:10 a.m. on January 30, 2020.

17. On February 3, 2020, a U.S. Postal Inspector interviewed hotel management at the Hyatt Place Hotel. The hotel manager indicated she remembered the subject parcel and the interaction with a guest attempting to claim it. The hotel manager stated a room had been reserved by GRAVES for one night, checking in January 30, 2020, and checking out January 31, 2020. At the time the subject parcel was delivered there was no guest by the name “Jasmin William” staying at the hotel. The hotel manager said shortly after the subject parcel was delivered, GRAVES called the front desk and added the name “Jasmine Williams” as a guest to her room. The hotel manager did not recall when the parcel was actually picked up or who retrieved it.

18. On February 6, 2020, investigators from the USPIS, DEA and HSI established surveillance on GRAVES’ residence, **Subject Premises 2**, after discovering that another package suspected of containing narcotics was being delivered to the Hyatt Place Hotel. That same day, investigators were able to observe GRAVES leave **Subject Premises 2** in a dark blue 2019 GMC Acadia bearing Ohio registration number GNL2992. This 2019 GMC Acadia is registered to Acar Leasing LTD and additional owner Niesha GRAVES at **Subject Premises 2**. Investigators followed GRAVES to the Hyatt Place Hotel, where they observed her check in at the front desk, retrieve the package, exit the hotel and return to **Subject Premises 2**.

19. On March 4, 2020, a postal inspector conducted surveillance at 3834 Lamarque Court, Columbus, Ohio, to observe whether a package that was delivered that morning had been sent from the same postal account as other suspect packages. When the inspector arrived, there were no vehicles in the designated parking space for the residence. At approximately 10:56 a.m., a maroon Volkswagen sedan (OH license plate HXQ 2849) stopped directly in front of 3834 Lamarque Court. While the vehicle was still running, a

black male (later identified to be DIRKE) exited the driver's seat of the vehicle and climbed the stairs toward the residence. About two minutes later, the same black male was observed walking down the stairs with an object tucked under his left arm. Using binoculars, the inspector saw the object was a white USPS Priority Mail Express envelope or padded mailer. The black male placed the envelope into the passenger side of the vehicle, reentered the driver's side and departed the area.

20. The maroon 2013 Volkswagen Passat bearing Ohio registration plate HXQ2849 is registered to Brandon DIRKE at 3834 Lamarque Court, Columbus, Ohio, and upon reviewing the photograph of DIRKE attached to the Ohio Bureau of Motor Vehicles registration, the inspector confirmed the black male driving the vehicle was DIRKE.

21. On March 17, 2020, investigators observed DIRKE drive to **Subject Premises 2**. Jasmine Williams (WILLIAMS) was observed exiting the **Subject Premises 2**, and entering DIRKE's vehicle with no audible or visible signal being given by DIRKE that he had arrived. Agents believe DIRKE likely used a cellular telephone to call or text the occupants of **Subject Premises 2** that he had arrived. After a short period of time, WILLIAMS exited the vehicle and re-entered **Subject Premises 2**. WILLIAMS was previously identified by agents through Ohio Bureau of Motor Vehicle records detailing individuals residing at **Subject Premises 2**.

22. Postal inspectors have been able to determine several packages have been sent from the targets in Arizona to 3834 Lamarque Court, Columbus, Ohio. DIRKE lists 3834 Lamarque Court, Columbus, Ohio as his address of residence for his Ohio Operators License, and vehicle registrations. Surveillance has shown, however, that DIRKE resides at **Subject Premises 1**, and that his brother lives at the Lamarque Court address. DIRKE has been consistently present at **Subject Premises 1** during the days and nights since that address was identified in the investigation. On two different dates Agents have observed DIRKE return to **Subject Premises 1** immediately after picking up packages sent by

BARNHILL to an 1812 Minnesota Avenue address (as described further below). Agents found DIRKE has associated the Minnesota Avenue address with his Experian Credit Report in 2019. On both occasions, DIRKE either used a key to enter the front door, or walked directly into **Subject Premises 1**. Due to the nature of the location and the risk of being identified, Agents were unable to verify whether DIRKE brought the package inside the residence.

23. Though the investigation, agents have learned that BARNHILL is another individual mailing packages containing narcotics for MCCOY and livedabs, and has been identified by agents in Arizona through Driver's License photographs. Agents in Arizona have observed MCCOY and BARNHILL interacting with each other at both MCCOY and BARNHILL's residences and BARNHILL sometimes travels directly to a post office after meeting with MCCOY.

24. On March 23, 2020, investigators observed DIRKE arrive at **Subject Premises 2**. DIRKE knocked on the front door, spoke briefly to the person who answered the door before the door was closed again. A few minutes later, someone else opened the door and after briefly speaking, DIRKE took what appeared to be U.S. currency (about the size of a baseball) from his jacket pocket and handed it to a person inside **Subject Premises 2**. DIRKE then left the area.

25. On March 17, 2020, April 3, 2020, and April 7, 2020, investigators observed GRAVES drive to the post office located at 6400 Emerald Parkway, Dublin, Ohio, and mail packages believed to contain U.S. currency (due to the size and weight) to recipients at 2318 South Country Club Drive, Mesa, Arizona 85210. According to agents in Arizona who are surveilling MCCOY, MCCOY is frequently seen at this address. The packages GRAVES mailed used EasyPost mailing labels and were not intercepted.

26. Your Affiant knows from previous training, experience, and seizures that the type of electronic postage affixed to the subject parcel noted above is associated with illegal

Dark Web activity. The postage meter used to purchase this electronic postage is currently leased by the USPS to a shipping company doing business as EasyPost. EasyPost then subleases this particular meter to a company doing business as Bitcoinpostage.info. Bitcoinpostage.info sells USPS postage in exchange for bitcoin payment allowing users to anonymously purchase postage and print mailing labels. The ability to purchase USPS postage using bitcoin, a form of electronic currency, is appealing to individuals involved in the sale and distribution of controlled substances on dark web marketplaces because it allows for the purchase of this postage without having to first convert funds to US currency.

27. On January 7, 2020, GRAVES sent a package similar to the ones sent on the above dates. That package was intercepted by investigators in Arizona. A United States Magistrate Judge in Arizona authorized a search warrant to open the package, which was found to contain \$16,600.00 in U.S. currency. The money was packaged similarly to how packages containing narcotics are packed by this organization—in vacuum sealed bags containing a yellow and white substance smelling like Bengay. Postal inspectors repackaged the currency and delivered it to its intended destination in Chandler, Arizona. An inspector in Arizona observed MCCOY arrive in a car that was being driven by a female resembling REMPEL, and pick up the package.

28. On April 13, 2020, Your Affiant observed DIRKE receive a 13-pound package that was mailed from Arizona to 1812 Minnesota Avenue, Columbus, Ohio. After DIRKE retrieved the package, he was followed to **Subject Premises 1**. Agents observed DIRKE enter **Subject Premises 1** but due to the nature of the location and the risk of being identified, were unable to verify whether DIRKE brought the package into **Subject Premises 1**. A few hours later DIRKE drove to **Subject Premises 2** where a female from DIRKE's vehicle met with GRAVES outside **Subject Premises 2**. DIRKE again gave no audible or visible indication to GRAVES of his arrival. Both GRAVES and the unknown

female, who was carrying a large purse, went inside **Subject Premises 2** and the unknown female exited still carrying the large purse, a very short time later returning to DIRKE's vehicle before they both left the area.

29. Later that day, GRAVES drove to the Post Office in Dublin and sent a package using a computer-generated EasyPost mailing label, resembling other packages that GRAVES has sent in the past. The package was intercepted by agents in Arizona, a search warrant was obtained, and agents discovered the package contained over \$40,930.00 in U.S. Currency.

30. On April 14, 2020, Your Affiant obtained State of Ohio search warrants to place a GPS tracking device on the maroon 2013 Volkswagen Passat. Since that time, Your Affiant has observed DIRKE receive packages from the targets in Arizona. Specifically, packages were mailed on May 4 and May 5, 2020, from Arizona to DIRKE at an address that the investigation has shown to be affiliated with DIRKE. BARNHILL was captured on surveillance video mailing the package on May 4.

31. On May 5, 2020, Your Affiant conducted surveillance of DIRKE and observed him driving in the direction of **Subject Premises 2**. Your Affiant took a position of observation approximately 200 yards from **Subject Premises 2**, in a separate apartment complex shortly before DIRKE's arrival to the area. At approximately 3:59 PM, Your Affiant observed DIRKE pull into the parking lot and stop in front of **Subject Premises 2**. GRAVES exited **Subject Premises 2** and stared in the direction of where Your Affiant was parked. DIRKE did not give an audible or visible notification of his arrival to GRAVES that Your Affiant could see or hear. GRAVES went to the passenger window of DIRKE's vehicle, and after a short conversation walked back to **Subject Premises 2**, staring again in the direction where Your Affiant was parked. DIRKE then drove from the parking lot and into the apartment complex where Your Affiant was parked, parked behind Your Affiant and walked up to the passenger side of Your Affiant's vehicle looking inside. DIRKE

returned to his vehicle and stayed parked behind Your Affiant for a few more minutes. DIRKE then drove around the area, before parking in a location to watch Your Affiant's vehicle. Your Affiant could see that someone inside **Subject Premises 2** was peeking out between the blinds while DIRKE was watching Your Affiant. When Your Affiant left his parking spot approximately 20 minutes later, DIRKE was observed trying to follow Your Affiant through a neighborhood. According to the data obtained from the state vehicle tracking warrant, DIRKE drove around the area for approximately 10 more minutes before returning home to **Subject Premises 1**.

32. On June 19, 2020, investigators in Arizona notified Your Affiant that a package had been shipped by BARNHILL addressed to "Brundon Dirk 1812 Minnesota Avenue, Columbus." The package was tracked through the USPS and was scheduled to be delivered on June 22, 2020. On June 22, surveillance was conducted on 1812 Minnesota Avenue. Your Affiant observed a white Jeep Wrangler arrive and park in front of 1812 Minnesota Avenue around the time the package was due to be delivered. The driver never exited the vehicle, but was later identified to be DIRKE. Upon delivery of the package an unknown person exited 1812 Minnesota Avenue and got into the passenger side of the Jeep with the package before leaving the area. A short time later, the Jeep was observed arriving at **Subject Premises 1**. Agents observed DIRKE exit the driver's door of the vehicle and entered **Subject Premises 1** through the front door without knocking. The passenger waited outside. A short time later DIRKE exited **Subject Premises 1**, and both left the area in another vehicle, leaving the Jeep behind at **Subject Premises 1**.

33. On June 22, 2020, DEA investigators in Arizona conducted surveillance of BARNHILL. They observed BARNHILL drive to the known residence of MCCOY, and carry shipping supplies from his car into the residence. A short time later BARNHILL exited the residence carrying two brown boxes, and then went back inside the residence and retrieved two envelopes, all of which he placed in his vehicle. BARNHILL was then

followed to the Scottsdale Main Post Office where he was observed taking all of the packages inside the Post Office. Once BARNHILL left the area, investigators with the help of the USPS Supervisor were able to identify and secure the four packages. One of the packages was addressed to “Brendon Dirk, 3834 Lamarque Court, Columbus, Ohio 43232-4954,” and weighed 10 pounds. All four packages contained the same return address of: “GIFT-ODOLOGY 16495 N SCOTTSDALE RD SCOTTSDALE AZ 85254.” Law enforcement in Arizona spoke to the owner of Gift-Ology, who stated that their business uses Pitney Bowes and not Easy Post prepaid shipping labels for its packages, that its return labels always say “Gift-Ology Scottsdale” and list their suite number. The owner also stated the business did not mail any packages from the Scottsdale Mail Post Office on June 22, 2020. On June 25, 2020, an email address, bdirke@yahoo.com, checked the tracking history on the parcel that was seized on June 22, 2020, in particular the above-described parcel addressed to “Brendan Dirk.”

34. USPS records indicate 32 other packages have previously been delivered to 3834 Lamarque Court, and 17 packages have been delivered to 1812 Minnesota Avenue from Arizona, all using the same EasyPost account with computer-generated labels as the seized package. Investigators believe these addresses are being used to protect the identities of the true recipients, and avoid detection by law enforcement.

35. A United States Magistrate Judge in Arizona authorized the search of all four of the above-described parcels and all four were found to contain illegal drugs. Specifically, the package addressed to DIRKE at 3834 Lamarque Court contained 3,542 grams of methamphetamine, and nine grams of a brownish/white powder that generated an inconclusive reading on the TruNarc device, but which agents suspect to be fentanyl, based on their training and experience.

36. Your Affiant is familiar with “Dark Web” narcotics traffickers, and the methods used by these traffickers to ship narcotics through the mail. Your Affiant knows

that “Dark Web Vendors” use individuals in several locations to re-ship narcotics to customers to avoid detection by law enforcement. Your Affiant believes that GRAVES, and DIRKE are re-shippers for MCCOY, and that DIRKE is picking up packages containing narcotics, collecting U.S. Currency from customers purchasing narcotics, and dropping illegal narcotics proceeds off to GRAVES, who sends the proceeds to MCCOY or other DTO members through U.S mail. Your Affiant knows that individuals working for “Dark Web Vendors” communicate with the vendor using electronic devices, and other co-conspirators through text messages, emails, phone calls, and encrypted messaging applications. They also use electronic devices such as computers, and cellular phones to access the Dark Web, purchase mailing labels, and track packages containing either U.S. Currency or illegal narcotics. Your Affiant also knows that individuals involved in receiving narcotics packages for “Dark Web Vendors” are known to store the narcotics in their residences prior to distributing the narcotics locally, or re-shipping the narcotics through package delivery services, and keep packaging material and shipping information for both packages received and shipped.

IV. ITEMS TO BE SEIZED

37. Based upon the facts contained in this Affidavit, Your Affiant submits there is probable cause to believe that the items listed in **Attachment A** will be found at the **Subject Premises 1 and 2**.

38. In addition, based on my training, education, and experience, and discussions with other trained law enforcement personnel, along with information provided by sources of information and confidential sources, Your Affiant knows the following:

a. Drug traffickers often keep large amounts of United States currency on hand in order to maintain and finance their ongoing trafficking activities. Traffickers commonly maintain such currency where they have ready access to it, such as in their homes and vehicles. It is also common for traffickers to possess drug proceeds and items

purchased with proceeds in their homes and vehicles. Thus, it is common for currency, expensive jewelry, precious metals, or financial instruments to be found in the possession of drug traffickers.

b. Traffickers and persons involved in the manufacturing, distribution, and possession of controlled substances often possess firearms and other weapons, both legal and illegal, in order to protect their person, drugs, or the proceeds of drug transactions. Traffickers commonly maintain such firearms and weapons where they have ready access to them, such as on their person, in their homes, and in their vehicles. In addition, other firearms-related items, such as gun pieces, ammunition, gun cleaning items or kits, holsters, ammunition belts, original box packaging, targets, expended pieces of lead, photographs of firearms, and paperwork showing the purchase, storage, disposition, or dominion and control over firearms, ammunition, and related items are commonly possessed by drug traffickers along with their firearms.

c. Traffickers often maintain paraphernalia for manufacturing and distributing controlled substances, including packaging materials, scales, and cutting agents. Traffickers commonly maintain such paraphernalia at stash houses, in their homes, or in their vehicles.

d. Traffickers often maintain paper records of their drug trafficking and money laundering activities. Your Affiant knows that such records are commonly maintained for long periods of time and therefore are likely to be found at **Subject Premises 1 and 2**.

e. Drug traffickers commonly use computers, cellular telephones, and other electronic devices to communicate with other drug traffickers and customers about drug-related activities through the use of telephone calls, text messages, email, chat rooms, social media, and other internet- and application-based communication forums. Moreover, drug traffickers—particularly those using the Dark Web—commonly use other capabilities

of computers and electronic devices to further their drug trafficking and money laundering activities. Therefore, evidence related to drug trafficking activity and money laundering activity is likely to be found on electronic storage media found at the **Subject Premises 1 and 2**, as further described below.

39. In addition to items which may constitute evidence, fruits and/or instrumentalities of the crimes set forth in this Affidavit, Your Affiant also requests permission to seize any articles tending to establish the identity of persons who have dominion and control over the **Subject Premises 1 and 2**, including rent receipts, utility bills, telephone bills, addressed mail, personal identification, keys, purchase receipts, sale receipts, photographs, vehicle pink slips, and vehicle registration.

V. DIGITAL EVIDENCE STORED WITHIN ELECTRONIC STORAGE MEDIA

40. As described in Attachment A, this application seeks permission to search for records that might be found in or on **Subject Premises 1 and 2**, in whatever form they are found, including data stored on a cellular telephone. Thus, the warrant applied for would authorize the seizure of all cellular telephones found in or on the **Subject Premises 1 and 2** and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

41. *Probable cause.* Your Affiant submits that if electronic storage media are found in or on the **Subject Premises**, there is probable cause to believe records and information relevant to the criminal violations set forth in this Affidavit will be stored on such media, for at least the following reasons:

a. Your Affiant knows that when an individual uses certain electronic storage media, the electronic storage media may serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage media is an instrumentality of the crime because it is used as a means of

committing the criminal offense. The electronic storage media is also likely to be a storage medium for evidence of crime. From my training and experience, Your Affiant believes that electronic storage media used to commit a crime of this type may contain: data that is evidence of how the electronic storage media was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

b. Based on my knowledge, training, and experience, Your Affiant knows that electronic storage media contain electronically stored data, including, but not limited to, records related to communications made to or from the cellular telephones, such as the associated telephone numbers or account identifiers, the dates and times of the communications, and the content of stored text messages, e-mails, and other communications; names and telephone numbers stored in electronic “address books;” photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system (“GPS”) information.

c. Based on my knowledge, training, and experience, Your Affiant knows that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on an electronic storage medium, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten.

In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. As previously set forth in this Affidavit, the targets of this investigation have used both computers and cellular telephones to send text messages, emails, phone calls, and encrypted messaging applications. They also use electronic devices such as computers, and cellular phones to access the Dark Web, purchase mailing labels, and track packages containing either U.S. Currency, or illegal narcotics. Therefore, Your Affiant believes that evidence of criminal activity will be found on any electronic storage media found at the **Subject Premises 1 and 2** and that the electronic storage media constitute instrumentalities of the criminal activity.

42. *Forensic evidence.* As further described in Attachment A, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be found on any electronic storage media located in or on the **Subject Premises 1 and 2** because:

a. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." Operating systems can record additional information, such as the attachment of peripherals,

the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. File systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the owner. Further, activity on an electronic storage medium can indicate how and when the storage medium was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on an electronic storage medium may both show a particular location and have geolocation information

incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the existence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera) not previously identified. The geographic and timeline information described herein may either inculcate or exculpate the user of the electronic storage medium. Last, information stored within an electronic storage medium may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage medium evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one electronic storage medium is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic storage medium was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish

that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

43. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on electronic storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine electronic storage media to obtain evidence. Electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that

might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the electronic storage media off-site and reviewing it in a controlled environment allows for a thorough examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats that may require off-site reviewing with specialized forensic tools.

44. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which Your Affiant is applying would permit seizing, imaging, or otherwise copying electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

45. Because several people share **Subject Premises 1 and 2** as a residence, it is possible that **Subject Premises 1 and 2** will contain electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those electronic storage media, the warrant applied for would permit the seizure and review of those items as well.

VI. CONCLUSION

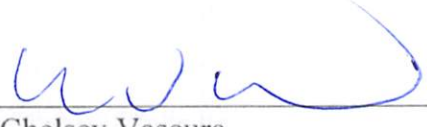
46. Your Affiant submits there is probable cause to believe that the items listed in Attachment A, which constitute evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1956 (Laundering of Monetary Instruments and Conspiracy to Launder

Monetary Instruments), 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute a Controlled Substance), 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance), 21 U.S.C. § 856 (Maintaining a Drug-Involved Premises), and 21 U.S.C. § 843(b) (Use of a Communication Facility to Commit a Federal Drug Felony), are likely to be found at the **Subject Premises 1 and 2**, which is further described in Attachment A.



TFO ANDREW WUERTZ
DRUG ENFORCEMENT ADMINISTRATION

Subscribed to electronically and sworn to telephonically this 26 day of June, 2020.



HONORABLE Chelsey Vascara
United States Magistrate Judge

ATTACHMENT A

Property to be seized

1. Any illegal controlled substances;
2. Books, records, receipts, notes, ledgers, invoices, and any other documentation related to the manufacture, importation, transportation, ordering, purchase, sale, or distribution of controlled substances;
3. Drug ledgers, drug customer lists, drug inventory lists, weights and prices, dealer lists, criminal associates lists, or any notes containing the individual names of such persons, telephone numbers or addresses of these customers or dealers, and any records of accounts receivable, money paid or received, drugs supplied or received, cash received, or to be paid for controlled substances, or intended to be paid for controlled substances;
4. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;
5. United States currency, foreign currency, financial instruments, negotiable instruments, jewelry, precious metals, stocks, bonds, money wrappers, and receipts or documents regarding purchases of real or personal property;
6. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;
7. Currency counters;

8. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and any vehicles found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records;
9. Photographs, including still photos, negatives, slides, videotapes, and films, in particular those showing co-conspirators, criminal associates, U.S. currency, real and personal property, firearms, or controlled substances;
10. Paraphernalia related to the importation, transportation, use, or distribution of controlled substances or proceeds from the sale of controlled substances, including materials commonly used for the clandestine shipment thereof, including but not limited to, scales, bottles, mixing bowls, spoons, grinders, cutting agents, cutting boards, baggies, knives/razors, plastic wrap/cellophane, tape, seals, boxes, packaging materials, scent masking agents, shipping labels, and storage containers;
11. Firearms, ammunition, magazines, cases, boxes, holsters, slings, gun pieces, gun cleaning items or kits, ammunition belts, original box packaging, targets, expended pieces of lead, and records, receipts, or other paperwork showing the purchase, storage, disposition, or dominion and control over firearms and ammunition.
12. Computers, cellular telephones, tablets, and other media storage devices, such as thumb drives, CD-ROMs, DVDs, disks, memory cards, and SIM cards (hereafter referred to collectively as “electronic storage media”);
13. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

14. Any records and information found within the digital contents of any electronic storage media seized from the Subject Premises, including:
 - a. all information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of drugs, drug packaging, and weapons;
 - b. all information related to buyers or sources of drugs or weapons (including names, addresses, telephone numbers, locations, or any other identifying information);
 - c. all bank records, checks, credit card bills, account information, or other financial records;
 - d. all information regarding the receipt, transfer, possession, transportation, or use of drug or firearm proceeds;
 - e. any information recording schedule or travel;
 - f. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;
 - g. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use, and events relating to crime under investigation and to the electronic storage media user;
 - h. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;

- i. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;
- j. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;
- k. evidence of the times the electronic storage media were used;
- l. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;
- m. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;
- n. records of or information about Internet Protocol addresses used by the electronic storage media;
- o. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- p. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored

communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from “apps,” including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the DEA may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.